

مهدی رشنو
 علی، تهران - مدتی است وقتی می‌خواهم از قسمت **run** وارد **msconfig** شوم، سیستم ناگهان ریست می‌شود و وقتی می‌خواهم وارد رجیستری سیستم شوم، با پیغام زیر روبرو می‌شوم:

redgistry edition has been disabled by your administrator

و سپس سیستم ریست می‌شود.

کنترل کنید که آیا Task Manager شما فعال است؟ اگر فعال است، Process‌های سیستم را کنترل کنید. در صورتی که در مورد Task Manager هم همان پیغام را داد، سیستم شما آلوده به ویروس شده است. برای شروع از برنامه Autorun Eater استفاده کنید تا Regisit و Task Manager شما فعال شود. سپس یک برنامه ضد ویروس به روز نصب کنید.

چگونه می‌توان فایل‌های pdf را باز کرد؟

برای مشاهده فایل‌های PDF (Portable Document File) می‌توانید از نرم‌افزار Acrobat reader محصول شرکت ادوب استفاده کنید. پس از نصب این نرم‌افزار، با باز کردن فایل‌های PDF. ویندوز فایل را با این نرم‌افزار باز می‌کند و محتویات آن را که به صورت متن، تصویر یا لینک است، به شما نشان می‌دهد.

پروانه پارسا - مدتی است کرم Recycled Virus در کامپیوترم هست که ضد ویروس‌های مختلف هم آن را نمی‌شناسند و به دلیل این که کرم است و نه ویروس، هر قدر آن را شیفت ذلیت می‌کنم، باز هم وقتی چیزی را حذف می‌کنم و یا Rar می‌کنم، می‌آید. می‌خواستم بپرسم که چطور بدون ضد ویروس می‌توانم آن را از بین ببرم؟

۱- سیستم را در حالت Safemode روشن کنید.

۲- به خط فرمان بروید و در شاخه C دستورات زیر را بنویسید.

۳- H -R -S AUTORUN.INF - ATTRIB سپس کلید Enter را بزنید.

۴- DEL AUTORUN.INF سپس Enter را بزنید.

۵- ATTRIB -H -R -S Recycled - سپس Enter را بزنید.

۶- پنجره Mycomputer در ویندوز (Safemode) را باز کنید و به درایو C بروید. پوشه Recycled را با کلیدهای

Shift+del پاک کنید.

۷- مراحل ۳ تا ۶ را برای تمام درایوهایتان (از جمله USB) تکرار کنید.

۸- در سیستم‌تان به دنبال EXE. CTFMON بگردید (با استفاده از Search در منوی Start). چنانچه فایلی

آشنایی با فناوری NetMasks و NAT

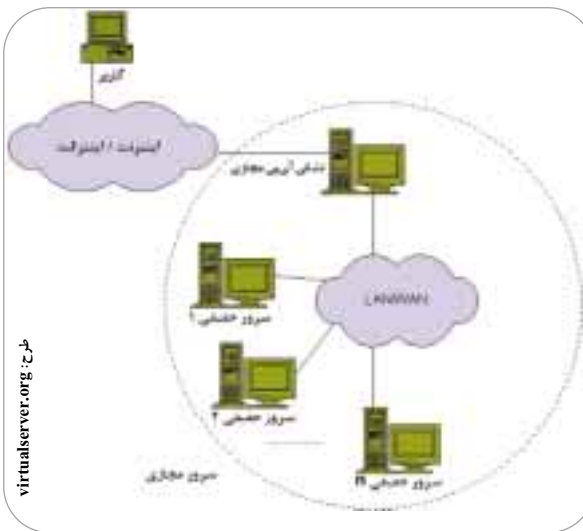
برای به کارگیری NAT یک دروازه Gateway میان شبکه با آدرس‌های غیرقانونی یا کنار گذاشته شده و اینترنت قرار می‌گیرد. یک دروازه می‌تواند آدرس‌ها را برای NAT از راه‌های مختلفی مثل نگاشت به آدرس‌های بی‌مفرد خارجی - نگاشت یک به یک و آدرس‌های تخصیص داده شده به صورت پویا نگاشت کند. همچنین مدیران شرکت‌ها و شبکه‌هایی که چندین کامپیوتر در سازمان خود دارند و نمی‌توانند برای همه آنها چندین آدرس آی‌پی مجاز و Valid خریداری کنند می‌توانند از فناوری NAT استفاده کرده و تنها با داشتن یک آدرس آی‌پی مجاز اینترنت را برای کلیه کامپیوترهایی که داخل

شبکه هستند، برقرار کنند. در این صورت آدرس آی‌پی تمامی کامپیوترها به صورت یک محدوده آی‌پی نامعتبر یا Invalid تنظیم شده و تمامی آنها به هنگام ارتباط با اینترنت از آدرس آی‌پی سرویس دهنده NAT استفاده می‌کنند. بنابراین فناوری NAT هم از لحاظ امنیتی بسیار موثر است و هم از لحاظ مالی استفاده از آن به صرف مدیران شبکه شده است.

درکل NAT امروزه در اینترنت به طور معمول استفاده می‌شود و هرکجا هنگامی که قادر نیستند بسته‌ها را به آدرس‌های غیرقابل مسیریابی روی شبکه داخلی بفرستند ممکن است آنها را از درون دروازه NAT بفرستند و دروازه NAT آدرس‌ها را به نمایندگی از مهاجم نگاشت خواهد کرد. بنابراین اگر قرار است شبکه ایمنی داشته باشیم و از آن حفاظت کنیم بهتر است تکنیک‌های NAT با سرویس Firewall ترکیب شود و هر دو با هم استفاده شوند.

منابع

www.experts-exchange.com
www.cert.org
www.virtualserver.org



بهر روز کمالیان
 هر آدرس IP به صورت واقعی از دو قسمت تشکیل شده است. آدرس شبکه و آدرس میزبان روی همان شبکه خاص. آدرس شبکه محلی (Lan) خاصی را توضیح می‌دهد که ترافیک می‌تواند برای رسانیدن بسته هدایت شود و آدرس میزبان ماشین مخصوص روی شبکه محلی داده شده را توضیح می‌دهد.

پرسشی که در اینجا پیش می‌آید، این است که چگونه کامپیوتر و یا مسیریاب می‌داند که کدام قسمت از آدرس آی‌پی مربوط به شبکه و کدام مربوط به میزبان است؟

استفاده از عملگر XOR تشخیص دهید. در مثال زیر تخمین آدرس شبکه را با استفاده از آدرس و Netmask IP مشاهده می‌کنید:

سوال دیگری که خیلی از علاقه‌مندان به شبکه می‌پرسند این است که مدیران شبکه‌ها چگونه دستیابی به اینترنت را از شبکه‌ای که از آدرس‌های غیرقانونی و یا کنار گذاشته شده استفاده می‌کنند، پشتیبانی می‌کنند؟ جواب این سوال هم این است که این آدرس‌های مشکلدار را با عمل Map یا نگاشت آدرس‌های آی‌پی در مسیریاب شبکه فایروال با استفاده از تکنیکی که Network Address Translation نام دارد، معتبر و قانونی می‌گردند.

پاسخ این سوال این است که چون اطلاعات پایه‌گذاری شده روی قسمتی که Netmask نامیده می‌شود، آن را تعریف می‌کند و به همین دلیل نت‌مسک مشخص می‌کند که کدام بیت‌ها در آدرس شبکه هستند و بقیه بیت‌های آدرس آی‌پی در قسمت میزبان واقع شده‌اند.

نت‌مسک عددی است که بیت‌های آن را وقتی که قسمتی از آدرس شبکه است به مقدار ۱ تنظیم می‌کند. وقتی که بیت داده شده در آدرس آی‌پی قسمتی از آدرس میزبان است، نت‌مسک دارای بیت صفر است. پس شما می‌توانید آدرس شبکه را با ترکیب ساده تمامی آدرس آی‌پی با نت‌مسک با

```
IP Address : 10.21.41.3 = 00001010 00010101 00101001 00000011
Netmask : 255.255.0.0 = 11111111 11111111 00000000 00000000
XOR -----
00001010 00010101 00000000 00000000
10.21.0.0 = آدرس IP شبکه
```

ضعف شما از دیدگاه یک مهاجم

پاراساستوده‌نیا

پیش از آن که سیستم‌های شبکه یا نرم‌افزارهای تحت وب ما مورد نفوذ یا حمله مهاجمان قرار گیرد بهتر است خودمان آن را از نظر امنیتی بررسی کنیم و تا حد امکان ضعف خود را پیش از آن که دیگران به آن پی ببرند، برطرف کنیم.

نرم‌افزار Core Impact pro، محصول Security technologies، یکی از پر استفاده‌ترین و قوی‌ترین نرم‌افزارهای ارزیابی امنیت شبکه و نرم‌افزارهای بر پایه وب است. این نرم‌افزار این کار را با استفاده از تکنیک‌های خاصی از جمله تکنیک‌هایی موسوم به Penetration testing برای شناسایی راه‌های نفوذ بهره می‌گیرد.

Penetration testing روشی برای ارزیابی امنیت یک سیستم رایانه‌ای یا شبکه با استفاده از شبیه‌سازی یک حمله توسط یک نفوذگر است. در واقع نرم‌افزار تلاش می‌کند تمام نقاط ضعف و مراکز نفوذ سیستم را پیدا کرده و آنها را آزمایش کند.

Core impact از معدود نرم‌افزارهایی است که به شما این امکان را می‌دهد تا امنیت شبکه یا برنامه تحت وب خود را از نگاه یک هکر ببینید. با استفاده از این برنامه می‌توانید آسیب‌پذیری‌های سرویس‌ها و سیستم‌عامل خود را در شبکه یا ایستگاه‌کاری به دقت استخراج کنید.

عمده نفوذگرها از ابزارها و روش‌های شناخته شده‌ای برای شروع کار خود استفاده می‌کنند و جالب این است که بسیاری از سیستم‌ها در برابر همین روش‌های شناخته شده نفوذگری ایمن نبوده و به سادگی آسیب‌پذیرند. نرم‌افزار Core impact علاوه بر این که راه‌های نفوذ متعارف را پیدا می‌کند، با استفاده از روش‌های خاصی می‌تواند نقاط احتمالی نفوذ و میزان آسیب‌پذیری هر نقطه را به دقت مشخص کند.

با وجود نرم‌افزاری نظیر core impact برای برقراری امنیت شبکه خود حتما نیاز به تخصص و تجربه در این زمینه نخواهید داشت. زیرا با به کارگیری فناوری‌های تست نفوذ امکاناتی در اختیار شما قرار داده می‌شود که می‌تواند امنیت کاملی برای سیستم شبکه سازمان یا موسسه خود برقرار سازد. برای اطلاعات بیشتر می‌توانید به سایت www.coresecurity.com مراجعه کنید.

